UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE RESIDENCE OF 53 WATSON ROAD, DOVER NH, A 2003 VOLVO 60 WITH NH REGISTRATION # 4629088 AND THE PERSON OF EVAN GADAROWSKI	))))))	**Case No. 1:21-MJ-** 42-01-AJ

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Derek Dunn, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant authorizing a search of the residence located at 53 Watson Road, Dover, New Hampshire (the "Premises"), a 2003 Volvo 60 bearing New Hampshire registration number 4269088 (the "Vehicle"), and the person of Evan Gadarowski ("GADAROWSKI"), as further described in Attachments A-1, A-2, and A-3. Located within the Premises, the Vehicle, and on GADAROWSKI's person, I seek to seize evidence, fruits, and instrumentalities of criminal violations which relate to the possession and production of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2251(a) and cyberstalking in violation of 18 U.S.C. § 2261A(2)(B) (the "Specified Federal Offenses"). Specifically, I request authority to search the entire Premises, including detached structures on the property and locked containers therein, the Vehicle, GADAROWSKI's person, and any computer and computer media located therein and to seize all listed in Attachment B as instrumentalities, fruits, and evidence of the Specified Federal Offenses.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been so employed since April 2003. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is almost entirely based on information conveyed to me by other law enforcement officials. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known by law enforcement officers concerning this investigation. While I have included all material facts relevant to the requested search warrant, I have not set forth everything known by officers about this matter.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of the Specified Federal Offenses have been committed by GADAROWSKI and that there is probable cause to believe that fruits, evidence, and instrumentalities of the Specified

Federal Offenses are likely to be found in the Premises, the Vehicle, and/or on GADAROWSKI's person, as set forth below.

SPECIFIED FEDERAL OFFENSES

6. Title 18 U.S.C. Section 2251(a) makes it a crime for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce.

7. Title 18, United States Code, Section 2252 makes it a crime for any person to, *inter alia*, knowingly possess one or more images depicting a minor under the age of 18 engaged in sexually explicit conduct.

8. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct;

or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

9. "Sexually explicit conduct" is defined by 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal . . .; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."

10. "Minor" means any person under the age of 18 years. 18 U.S.C. § 2256(1).

11. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

12. Title 18, United States Code, Section 2261A(2) holds that a person commits a violation of federal law if they "with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, use[] the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate commerce to engage in a course of conduct that . . . causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress."

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

13. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet

have revolutionized the manner in which child pornography is produced, possessed, distributed, and stored.

14. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking. With digital cameras, images of child pornography can be taken with or transferred directly onto a computer. In addition, the use of commercially available software and devices also allows for the conversion and transfer of other forms of visual media into various digital and electronic media formats. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

15. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. This is also true for portable electronic devices like cell phones and tablets.

16. The Internet affords individuals several different venues for meeting and communicating with each other; and obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. The Internet is also used as a means for child sexual exploitation offenders to solicit potential victims through the use of various online services to include, but not limited to, online profiles, email, instant messaging, and chat.

17. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in

"bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of files can be recovered months or years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer or portable electronic device, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

18. File transfers and online connections occur to and from IP (Internet Protocol) addresses. These addresses are unique to particular computers during online sessions. An IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

19. Third-party software is available to identify the IP address of a particular computer during an online session. Such software monitors and logs Internet and local network traffic. It is possible to identify the person associated with a particular IP address through Internet Service Provider records. ISPs maintain records of the IP addresses used by the individuals or businesses that obtain Internet connection service through the ISP. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

20. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Additionally, when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in

the warrant that authorizes the search. This sorting process can take days, weeks, or months, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

21. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

22. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. Sections 1470 and 2252, they should all be seized as such.

PROBABLE CAUSE

SNAPCHAT USERS TAYSNOW15 AND JAMIE.LIT

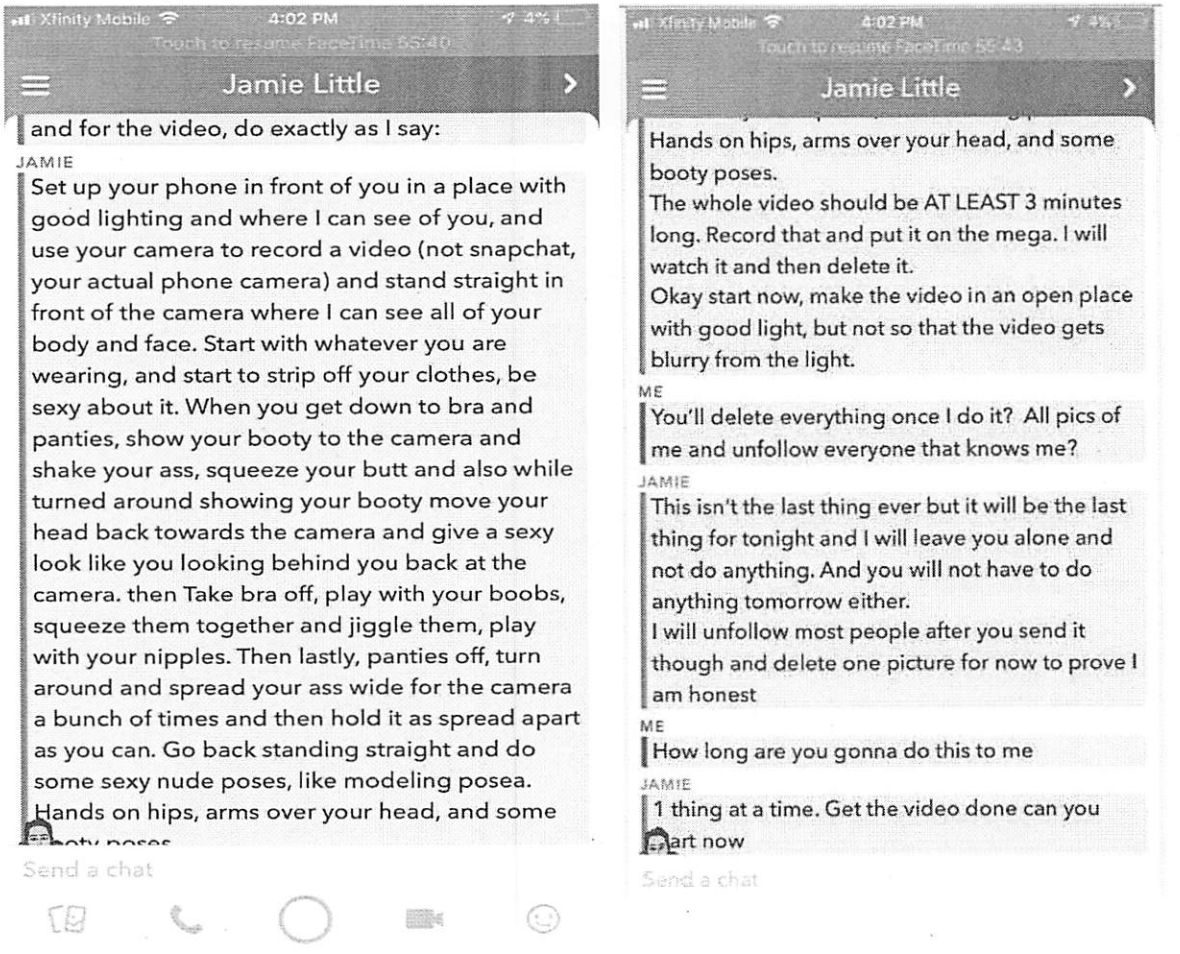
23. On or about December 12, 2018, a 14-year-old female ("Minor Victim #1"), filed a complaint with the Nashua, New Hampshire, Police Department regarding a person she knew as Taylor Snow. Minor Victim #1 initially said that she met Taylor Snow one year prior (January 2018) through a mutual friend. Minor Victim #1 subsequently admitted that she was in fact randomly messaged on the social media application Snapchat by Taylor Snow whose username was "TaySnow15."

24. Minor Victim #1 reported that she and "TaySnow15" became friends on Snapchat and Instagram and in 2018, Minor Victim #1 began sending images of her nude breasts to "TaySnow15." Minor Victim #1 believed that "TaySnow15" was a 16-year-old female lesbian. Minor Victim #1 admitted to sending at least five images to "TaySnow15" that showed her nude breasts and face. Minor Victim #1 explained that her communications with "TaySnow15" stopped after "TaySnow15" became, what she described as, obsessed with her.

25. Minor Victim #1 reported that on or about December 12, 2018, she was contacted by "TaySnow15" asking her if she had received a message from the Snapchat user "Jamie.Lit" threatening to "expose her if she did not comply." Immediately after receiving this message from "TaySnow15," Minor Victim #1 was contacted by "Jamie.Lit," who informed Minor Victim #1 to "do exactly" as he ordered or nude photographs of Minor Victim #1 would be released to her friends and family. When she asked what photographs he was referring to, Minor

Victim #1 was told they were the same ones of her breasts that she had sent "TaySnow15." "Jamie.Lit" then sent Minor Victim #1 one of the topless images that Minor Victim #1 had sent to "TaySnow15" as proof that he had possession of the images.

26. Minor Victim #1 reported that "Jamie.Lit" initially demanded clothed images of her which she did send. When she told him that she would "rather not" send him photos, he responded, "you have to, do you not understand? All of them and every picture of you." "Jamie.Lit" then progressed to requesting that she create and send him a sexually explicit video and gave her specific instructions on how to create it. The Nashua Police Department took screen captures of the conversation from Minor Victim #1's phone. Although the captures left out portions of the conversation, I have included portions below:



27. Minor Victim #1 said that she did not send the requested video. On December 13 or 14, 2018, Minor Victim #1 was able to capture the IP address being used by "Jamie.Lit" during one of their communications. She threatened to report him to the police. In response, "Jamie.Lit" listed the names of Minor Victim #1's friends, apparently threatening to send Minor Victim #1's photographs to those people. He continued, "you are not listening so you want to get sent" referring to sending out her topless photos.

28. Minor Victim #1 reported that she contacted "TaySnow15" and asked how "Jamie.Lit" came into possession of her images. "TaySnow15" stated that she recently lost her phone and the unknown person must have found it. Minor Victim #1 reported to Nashua Police Department that she believed that "TaySnow15" and "Jamie.Lit" were the same person.[1] Minor Victim #1 explained that she believed that "TaySnow15" was upset with Minor Victim #1 for no longer communicating and was now posing as "Jamie.Lit" to get back at her. She noticed that "TaySnow15" and "Jamie.Lit" never communicated with Minor Victim #1 at the same time and that "TaySnow15" and "Jamie.Lit" used similar wording in their communications with her.

29. On or about December 18, 2018, Minor Victim #1 reported the allegations against "Jamie.Lit" to Snapchat who in turn reported the information to the National Center for Missing and Exploited Children (NCMEC) ultimately resulting in NCMEC CyberTipline Report # 44423607 being generated.[2] The CyberTipline Report was forwarded to the Nashua Police Department (where Minor Victim #1's IP address geo-located) and the Dover, NH Police

[1] As will be discussed in more detail below, IP logs appear to confirm this.

[2] The National Center for Missing and Exploited Children's CyberTipline receives leads and tips from electronic service providers, internet service providers, and members of the public regarding suspected crimes of sexual exploitation committed against children. Tips sent through the CyberTipline generate a formal report, known as a "CyberTipline Report," which memorializes the tip, and often includes other pertinent information regarding the alleged sexual exploitation crime

Department (where the IP address Minor Victim #1 captured for "Jamie.Lit" geo-located) via the NH Internet Crimes Against Children Task Force.

30. Investigators received New Hampshire state search warrants for Snapchat accounts "TaySnow15", "Jamie.Lit", and the account used by Minor Victim #1. The "TaySnow15" account was created on 02/11/2018 with an associated email address of daniometahorn@gmail.com and the "Jamie.Lit" account was created on 10/21/2017 with an associated email address of lordofthespies@tutanota.com.

31. Based on the following chart showing activity for both accounts on 12/12/2018 and 12/13/2018, I believe that the same individual was using one electronic device to access both accounts based on the fact that the same IP addresses were used at the same time but neither account was logged into at the same time:

Date & Time (UTC)	Account	Activity	IP Address
12/12/2018 23:13:01	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:14:28	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:16:51	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:17:12	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:18:06	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:19:46	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:21:38	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:21:56	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:25:14	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/12/2018 23:25:39	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:14:58	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:15:36	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:19:22	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:19:51	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:21:03	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:21:45	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:25:07	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:25:36	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:26:34	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:27:02	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 00:28:33	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69

12/13/2018 00:28:55	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 01:17:23	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 01:18:01	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 01:19:23	taysnow15	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 01:19:45	jamie.lit	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 04:30:39	jamie.lit	Log off	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 04:31:12	taysnow15	Login	2601:187:8400:5c8:b176:4a42:8d67:4c69
12/13/2018 18:57:04	taysnow15	Log off	2600:1:f525:d5a:4d09:94b0:61ed:1ff2
12/13/2018 18:59:06	jamie.lit	Login	2600:1:f525:d5a:4d09:94b0:61ed:1ff2
12/13/2018 22:02:39	jamie.lit	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 22:03:08	taysnow15	Login	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 22:06:13	taysnow15	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 22:08:11	jamie.lit	Login	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 22:11:36	jamie.lit	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 22:11:58	taysnow15	Login	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:23:11	taysnow15	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:23:44	jamie.lit	Login	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:26:57	jamie.lit	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:27:52	taysnow15	Login	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:55:02	taysnow15	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:55:26	jamie.lit	Login	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:56:10	jamie.lit	Log off	2601:187:8400:5c8:1509:89fd:997d:d506
12/13/2018 23:56:46	taysnow15	Login	2601:187:8400:5c8:1509:89fd:997d:d506

32. IP address 2601:187:8400:5c8:b176:4a42:8d67:4c69 and 2601:187:8400:5c8:1509:89fd:997d:d506 are both registered to Comcast Cable Communications while IP address 2600:1:f525:d5a:4d09:94b0:61ed:1ff2 is registered to Sprint. In response to a Subpoena served to Comcast Cable Communications, the subscriber for IP address 2601:187:8400:5c8:1509:89fd:997d:d506 on 12/14/2018 at 06:03:14 UTC was J. Michael Joyal Jr. of 53 Watson Road Dover, NH (the Premises). Note that this is the date and time IP address 2601:187:8400:5c8:1509:89fd:997d:d506 was associated with the "TaySnow15" account as reported by Snapchat to NCMEC. This was the only IP address for which the Nashua Police Department requested subscriber records. Subpoenas were not served to Comcast for IP address

2601:187:8400:5c8:b176:4a42:8d67:4c69 or to Sprint for IP address 2600:1:f525:d5a:4d09:94b0:61ed:1ff2.

33. The search warrant returns also included numerous communications between "TaySnow15" and Minor Victim #1 from May 3, 2018 to December 13, 2018. Investigators were not able to find any communications during which Minor Victim #1 sent "TaySnow15" topless images of herself in these results. Also, based on a comparison of Minor Victim #1's screen captures to the data provided in response to the Snapchat Search Warrant, I believe that Snapchat did not retain and therefore did not provide some of the communications within these accounts. Within the "Jamie.Lit" account, investigators were unable to find much of the conversation in Minor Victim #1's screen captures.

34. The "TaySnow15" account contained communications between "TaySnow15" and other Snapchat users that appear to discuss trading sexually explicit photos and images of young girls. Specifically, on December 13, 2018, "TaySnow15" appeared to discuss his conversation with Minor Victim #1 with Snapchat username "Lancaster02468":

TaySnow15	"well shit got fucked up that girl is not gunna be doing anything and I am going to jail"
TaySnow15	"have fun"
Lancaster02468	"Why's girl?"
TaySnow15	"the girl I sent selfies of!!"
Lancaster02468	"Ana? Or who"
Lancaster02468	"And what happened?"
Lancaster02468	"The most recent girl%2C what happened?"
TaySnow15	"she got my IP address"
Lancaster02468	"How and what happened"
TaySnow15	"she sent me a link I thought it was the mega where she was sending the video%2C and she told me to leave her alone or she would tell the police"
TaySnow15	"I know she was just bluffing but still"
Lancaster02468	"Why you threatening her"
TaySnow15	"I wanted more stuff to send you :/"

35. I believe that in this conversation, "TaySnow15" is referring to his threatening of Minor Victim #1 to get her to create more images for "TaySnow15" to share with "Lancaster02468." In another conversation, "TaySnow15" discussed sharing what I believe to refer to child exploitation material with Snapchat username "OneKiddsam."

Onekiddsam	"No braces there either smaking there ass grabbing there boobs or fingering themselves?"
TaySnow15	"Oh"
Onekiddsam	"Yea I do send urs"
TaySnow15	"Link sent https://mega.nz/....
Onekiddsam	"Link sent https://www.dropbox.com/sh/....."
TaySnow15	"what about the other stuff%C nice....and boobs and face"
TaySnow15	"or just what else did you get since feb 17th lol"

36. I know that "mega.nz" and "dropbox" are file storage and sharing websites. Also in this conversation, "OneKiddsam" sent various images depicting apparent child sex abuse images to "TaySnow15."

37. The "TaySnow15" account contained several communications with young females from March through December of 2018. For example, on March 26, 2018, "TaySnow15" communicated with a Snapchat user whose screenname contained the name "Audrey" about using Snapchat to send images stating "so because I set up my phone and use my camera not Snapchat to record it I'd just like put in google drive I could make us our own email and password to privately keep stuff." "TaySnow15" provided "Audrey" with account name taybayandaudrey@gmail.com along with the password for the account. "TaySnow15" then instructed "Audrey" on how to create a sexually explicit video including in part, "then get down on the ground and spread your pussy with your fingers babe and play with your boobs more while you are on the ground..." Included in response to a New Hampshire state search warrant for the account taybayandaudrey@gmail.com was a 53 second sexually explicit video of a

pubescent Caucasian female with long black hair and orthodontic braces performing acts that are consistent with the request made by "TaySnow15" described above. The female has some signs of secondary female sex characteristics, minimal breast development, small muscular and bone structure, and facial features that are consistent with those of a teenage female approximately 14 to 16 years of age.[3]

38. On another occasion, "TaySnow15" created another personalized Gmail account tayyandchloe@gmail.com for a Snapchat user whose screenname contained the name "Chloe" and requested that "Chloe" send him sexually explicit videos, giving specific instructions for how to make the videos. According to returns from a New Hampshire state search warrant, the account contained seven sexually explicit videos of a pubescent Caucasian female believed to under the age of 18 based on her partially developed breasts, smaller bone structure and limited muscle tone. Utilizing information provided by Google and Snapchat, law enforcement officers identified a female in Michigan who matches the image in the photos and who was 16 years old at the time of the video uploads and communications and whose name is "Chloe."

39. Also within the search warrant response was an audio message from "TaySnow15" to "Lancaster02468" in which the voice of "TaySnow15" is clearly that of a male. The "TaySnow15" account also contained a video of a skinny white male in a motor vehicle. The male in the video appears to be GADAROWSKI based on a comparison of the photo to his New Hampshire driver's license.

[3] I have not reviewed the images of child pornography described in this affidavit. All of the descriptions have been provided to me by New Hampshire ICAC Task Force State Supervisor and HSI Task Force Officer Todd Faulkner who personally reviewed the images. Lieutenant Faulkner has been a member of the ICAC task force for many years and has participated in numerous child exploitation investigations. In his career, he has reviewed hundreds of images of child pornography and has received substantial training in child pornography investigations.

40. The "TaySnow15" account contained a video of a black Labrador dog with the background of what appeared to be a living room. A Facebook page for "Evan Gadarowski" of Dover, NH which contained photos of GADAROWSKI revealed a post dated September 15, 2016, in which GADARWOSKI reported the passing of his dog "Molly" and included a picture of an all black dog that appeared to be a Labrador. Town records, however, show that a different type of dog is owned by GADAROWSKI as of 2019.

SNAPCHAT USER JACKMULLENS2019

41. On January 15, 2020, NCMEC received information from Snapchat in CyberTipline Report # 62834374. The CyberTipline Report stated, "[t]his report was submitted by Snapchat concerning "ONLINE ENTICEMENT – BLACKMAIL. It appears the brother is reaching out on behalf of his 13-year-old sister who had sent nude photographs to a stranger and ended up getting blackmailed. CT/TA queries returned negative results." The suspect username was "jackmullens2019" and the suspect's IP address was identified as 67.189.134.8, registered to Comcast Cable Communications, on January 13, 2020, at 09:29:54 UTC. NCMEC forwarded the CyberTipline Report to the NH ICAC Task Force due to the suspect IP address geo-locating to Dover, New Hampshire. The CyberTipline Report also included four images that were uploaded to "jackmullens2019" by three different Snapchat users.

42. A review of all four of the images that Snapchat reported they had reviewed prior to submission to NCMEC, revealed two of apparent child pornography.

a. *chat~batched_media~1574293980240~allybat2004~jackmullens2019~saved~97DB519B-EBDB-4F84-9A41-A4436B0E5CFF~V4*: This is an image of a pubescent female, with some secondary female sex characteristics. This female has beginning stages of breast development and limited muscle tone and bone structure. She appears to be approximately 13-15 years of age. The female is wearing transparent negligee, on the floor kneeling and leaning forward holding her torso up by her elbows and her buttocks raised in the air. The female's

slightly developed breasts and nipple can be seen through the outer garment. This is a sexual pose and the photograph draws the viewers' attention to the female's breast and buttocks.

b. *chat~media_v4~1573363584554~emo_llama0211~jackmullens2019~saved~18CE000A-3769-4642-B5A4-65258DCBFAF8~V4*: This image displays a pubescent Caucasian female taking a "selfie" image with the camera in front of her face. She is seen kneeling on the floor with her legs spread while wearing black negligee style panties. The female is not wearing any other clothing, and her secondary female sex characteristics show her partially developed breasts, smaller bone structure and limited muscle tone. This is a sexual pose with the focal point of the image being the female's breasts and vaginal area. This female is approximately 15-17 years of age.

43. In response to a Subpoena, Comcast Cable Communications identified the subscriber for IP address 67.189.134.8 on January 13, 2020 at 09:29:54 UTC as J. Michael Joyal Jr. of the Premises.

44. In response to a New Hampshire state search warrant for Snapchat account "jackmullens2019," the following information was provided:

a. The account was created on 05/25/2019 at 4:48:45 PM and listed with a username of Jack Mullens.

b. The account is linked to email account taybayandmarissa@gmail.com and a phone number of 1-206-312-0919. I note that this Gmail account is consistent with others created by the "TaySnow15" account.

45. In response to a Subpoena, TextNow Incorporated provided information that the subscriber for phone number 1-206-312-0919 is Dannio Metahorn with an associated email address of daniometahorn@gmail.com. This is the same email address associated with "TaySnow15."

46. In addition, investigators reviewed communications between "jackmullens2019" and a female user who described herself as born on November 10, 2004, which would have made

her 15 at the time of the communications. In one of the conversations, she sent "jackmullens2019" the image described in Paragraph 42(a). The user also sent other photographs where the focal point of the image was on her vagina.

DANIOMETAHORN@GMAIL.COM

47. Investigators received a New Hampshire state search warrant for email address daniometahorn@gmail.com, associated with the subscriber information for Snapchat user "TaySnow15" and phone number 1-206-312-0919 which is associated with the subscriber information for Snapchat user "jackmullens2019."

48. In response to a New Hampshire state search warrant for the account daniometahorn@gmail.com, geo-location (longitude and latitude) coordinates associated with the device utilizing the account were provided for more than 248,000 timestamps during the period from July 15, 2018 through July 3, 2019. An analysis of these coordinates determined that the device utilizing the daniometahorn@gmail.com account was located at the Premises for more than 170,000 of these timestamps during that period of time. Furthermore, the device utilizing the daniometahorn@gmail.com account was located at the Premises for approximately 790 timestamps out of approximately 1,000 timestamps during the period from December 12, 2018, at 23:13:01 UTC to December 13, 2018, at 23:59:39 UTC which is the time frame previously described in this affidavit that Snapchat users "TaySnow15" and "Jamie.Lit" were communicating with Minor Victim #1.

49. Contained within the damiometahorn.@gmail.com account were 6 folders containing image and/or video files, each titled with the name of a female. Included in the files were images and videos of females that appear to be between the ages of 13 and 17 engaging in sexually explicit conduct.

THE PREMESIS

50. The Dover City Tax Map lists the property of 53 Watson Road, Dover, NH, the Premises, as owned by J. Michael L. Joyal Jr. and Kathleen Joyal Gadarowski. Based on surveillance conducted by law enforcement at the Premises between January 26, 2021, and February 10, 2021, the occupants believed to be residing at the residence are Michael L. Joyal Jr., Kathleen Joyal Gadarowski, GADAROWSKI, and possibly GADAROWSKI's 24-year-old sister who has been seen coming and going from the residence. During this time frame, GADAROWSKI was consistently observed leaving the residence and traveling in a Volvo bearing NH registration number 4629088 to his suspected place of employment, Stonewall Kitchens located in Dover, New Hampshire. According to the New Hampshire Department of Motor Vehicles, vehicle registration number 4629088 is issued to a 2003 Volvo 60 four door sedan owned by GADAROWSKI with the Premises listed as the registered address.

51. Although much of the activity discussed herein occurred in 2018 and 2019, and most recently on January 13, 2020, I believe that GADAROWSKI has lived in the Premises during most of if not all of the entire timeframe. As the evidence discussed herein indicates that during the over one-year period that is the focus of the affidavit, he engaged in the Specified Federal Offenses regularly, I believe it is likely that evidence of the crimes discussed herein is likely to still exist at the Premises, in the Vehicle, and/or on GADAROWSKI's person. As discussed previously, I know that electronic devices can store evidence for years and even if deleted by a user, that evidence can often be recovered by forensic examination. I also know that people tend to keep electronic devices including computers and cellular telephones for periods of time longer than one year and therefore that there is probable cause to believe that devices

containing evidence and/or used to commit the Specified Federal Offenses will still be in the premises to be searched.

BIOMETRIC ACCESS TO DEVICES

52. This warrant seeks authorization for law enforcement to compel GADAROWSKI to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

53. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

54. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

55. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on

certain Android devices and is called "Trusted Face". During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

56. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

57. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

58. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

59. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked fora certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

60. In light of the foregoing, and with respect to (1) any device found on the person of GADAROWSKI, or (2) any device at/on the Premises or Vehicle reasonably believed to be owned, used, or accessed by GADAROWSKI, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of GADAROWSKI to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of GADAROWSKI and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of GADAROWSKI and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

61. The proposed warrant does not authorize law enforcement to compel that an individual present at the Premises state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the Premises to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

62. Based on the aforementioned facts and circumstances, your Affiant respectfully submits that there is probable cause to believe that GADAROWSKI, who resides at the Premises and owns and operates the Vehicle, has violated the Specified Federal Offenses; and that the fruits, evidence, and instrumentalities of the Specified Federal Offenses are likely to be found in the Premises, in the Vehicle, and/or on GADAROWSKI's person.

63. Your Affiant, therefore, respectfully requests that a search warrant be issued authorizing the search of the Premises, the Vehicle, and GADAROWSKI's person as listed in Attachments A-1, A-2, and A-3 and the seizure of the items listed in Attachment B.

/s/ Derek Dunn
Special Agent Derek Dunn
Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me on this 2nd day of March, 2021.

Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A-1

DESCRIPTION OF THE PREMISES

The Premises, located at 53 Watson Road, Dover, NH, is a two story single family yellow residence with attached garage, shingled roof and white trim. The warrant authorizes the search of any outbuildings and safes or locked storage containers located in the Premises.

ATTACHMENT A-2

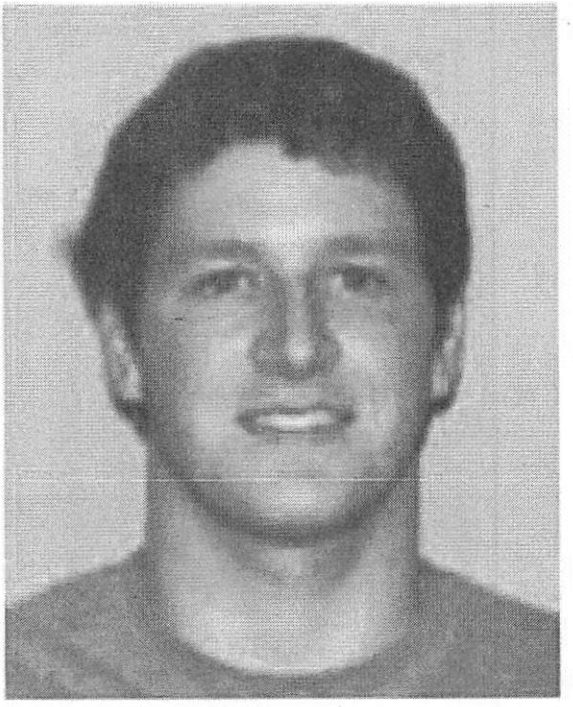
DESCRIPTION OF THE VEHICLE

The Vehicle is a green 2003 Volvo 60 sedan bearing New Hampshire registration number 4629088, registered to Evan Gadarowski of 53 Watson Road, Dover, NH

ATTACHMENT A-3

DESCRIPTION OF THE PERSON

The person of Evan Gadarowski, with an address of 53 Watson Road, Dover, NH (DOB 08/04/1994), height 5'10', weight 175 pounds, hair brown, and eyes blue, as described in his New Hampshire Driver's License number NHL11965099.



ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

1. All records relating to possession and production of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2251(a) and cyberstalking in violation of 18 U.S.C. § 2261A(2)(B) (the "Specified Federal Offenses") and images of child pornography and files containing images of child pornography in any form, wherever these items may be stored or found including, but not limited to:
    a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;
    b. records or information pertaining to an interest in child pornography;
    c. communications with minor children regarding engaging in sexually explicit conduct;
    d. records or information pertaining to the receipt of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
    e. records or information pertaining to use of the applications SnapChat, Instagram, and Gmail ;
    f. records or information relating to the occupancy or ownership of the Premises and electronic devices therein, including, but not limited to, utility and telephone bills, mail envelopes, vehicle registrations, tax bills, and other correspondence.

2. Any computer or electronic media that were or may have been used by GADAROWSKI as a means to commit the Specified Federal Offenses.

3. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

j. evidence of the crimes described above in paragraph 1 including but not limited to images of child pornography, the use of messaging applications like Skype, Gmail, and Instagram and specifically the accounts discussed in this affidavit, use of the IP addresses discussed in the affidavit, communications with minors, threats to minors, use of file sharing applications including but not limited to dropbox and mega, and communications with others with an interest in sharing child pornography.

4. Records and things evidencing the use of the Internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. DEVICE UNLOCK: During the execution of the search of the property described in Attachment A, and with respect to (1) any device on GADAROWSKI's person, or (2) any device at/on Premises reasonably believed to be owned, used, or accessed by GADAROWSKI, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of GADAROWSKI to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of GADAROWSKI and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the

face of that GADAROWSKI and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units,

acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or) signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).